PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-016596
(43)Date of publication of application : 18.01.2002

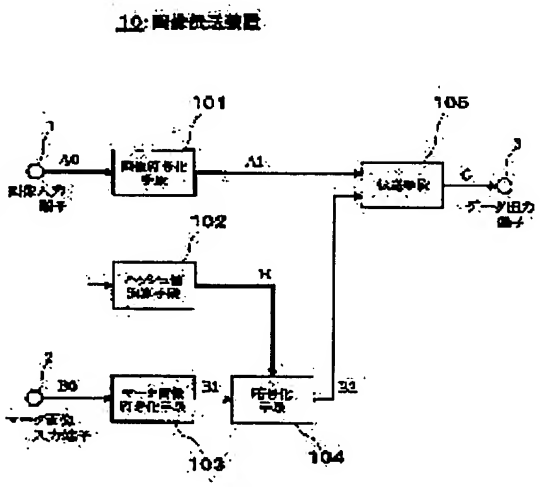
(51)Int.Cl. H04L 9/32
H04N 1/387
H04N 1/44

(21)Application number : 2000-195856
(22)Date of filing : 29.06.2000

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : MAENO KURATO

(54) IMAGE TRANSMITTER AND IMAGE RECEIVER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an image transmitter and an image receiver that can easily prevent falsifying of image data and enable the originaness of the image data to be confirmed visually.
SOLUTION: The image receiver 20 receives coded data A1 of an image and coded data B2 of an encrypted mark image that are transmitted from the image transmitter 10 and uses a hash value H of a decoded image A0 for decoding the encrypted mark image. The mark image B0, in combination with the image A0, is outputted. If even part of the image is falsified, the coded data of the mark image which is decoded by using the hash key for a key become one which differ from the coded data that have not been falsified. Thus, viewing the mark image of the image ultimately generated can be confirmed visually and easily as to whether the image has been falsified.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－16596
（P2002－16596A）
(43)公開日　平成14年１月18日(2002.1.18)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｎ　1/387		５Ｃ０７５
Ｈ０４Ｎ　1/387			1/44	５Ｃ０７６
1/44		Ｈ０４Ｌ　9/00	６７５Ａ	５Ｊ１０４

審査請求　未請求　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願2000－195856(P2000－195856)

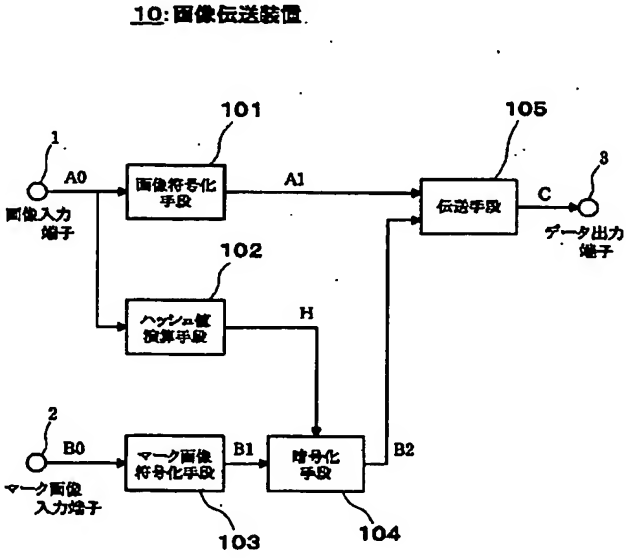
(22)出願日　平成12年６月29日(2000.6.29)

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号
(72)発明者　前野　蔵人
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(74)代理人　100095957
弁理士　亀谷　美明　（外３名）

Ｆターム(参考)　5C075 EE03 EE06
5C076 AA14 AA15 AA19 BA06 BA09
5J104 AA08 LA02 LA05 NA12

(54)【発明の名称】　画像伝送装置及び画像受信装置

(57)【要約】
【課題】　画像データの改竄を容易に防止でき，画像データの原本性を視覚的に確認することの可能な画像伝送装置及び画像受信装置を提供する。
【解決手段】　画像受信装置２０は，画像伝送装置１０より伝送された，画像の符号化データＡ１と，暗号化されたマーク画像の符号化データＢ２とを受信し，復号化された画像Ａ０のハッシュ値Ｈを用いてマーク画像の暗号解読を行う。マーク画像Ｂ０は画像Ａ０と結合されて出力される。画像の一部にでも改竄が行われた場合，そのハッシュ値をキーとして解読されたマーク画像の符号化データは，改竄が行われていない場合の符号化データとは異なったものとなる。このため，最終的に生成される画像のマーク画像を見れば，画像に改竄が行われたか否かを視覚的かつ容易に確認することができる。



【特許請求の範囲】
【請求項１】　画像伝送装置において，第１の画像を符号化する第１の画像符号化手段と，前記第１の画像のハッシュ値を計算するハッシュ値演算手段と，第２の画像を符号化する第２の画像符号化手段と，前記第２の画像の符号化データを，前記第１の画像のハッシュ値をキーとして暗号化する暗号化手段と，前記第１の画像の符号化データと前記暗号化された第２の画像の符号化データとを伝送する伝送手段と，を有することを特徴とする，画像伝送装置。
【請求項２】　前記伝送手段は，前記第１の画像の符号化データと前記暗号化された第２の画像の符号化データとを多重化する多重化手段を備えたことを特徴とする，請求項１に記載の画像伝送装置。
【請求項３】　前記第２の画像は，マークを含む印章あるいはサインの画像であることを特徴とする，請求項１または２に記載の画像伝送装置。
【請求項４】　画像受信装置において，第１の画像の符号化データと暗号化された第２の画像の符号化データとを受信する受信手段と，前記第１の画像の符号化データを復号する第１の画像復号化手段と，前記復号された第１の画像のハッシュ値を計算するハッシュ値演算手段と，前記暗号化された第２の画像の符号化データを，前記第１の画像のハッシュ値をキーとして解読する暗号解読手段と，前記解読された第２の画像の符号化データを復号する第２の画像復号化手段と，前記復号された第１の画像と前記復号された第２の画像とを結合する画像結合手段と，を備えたことを特徴とする，画像受信装置。
【請求項５】　前記受信手段は，前記第１の画像の符号化データと前記暗号化された第２の画像の符号化データとが多重化されている場合に，該多重化データを分離する多重化分離手段を備えたことを特徴とする，請求項４に記載の画像受信装置。
【請求項６】　前記第２の画像は，マークを含む印章あるいはサインの画像であることを特徴とする，請求項４または５に記載の画像受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は画像伝送装置及び画像受信装置にかかり，特に，画像データの改竄を防止し，原本性を保証することの可能な画像伝送装置及び画像受信装置に関する。
【０００２】
【従来の技術】近年，書類や請求書などを画像データとしてコンピュータに取り込み，電子メールシステムを用いてデータをやり取りするいわゆるペーパーレス対策を講じる企業が増加しつつある。しかしながら，近年におけるコンピュータ関連技術の発達は，かかるペーパーレス対策の一助となる一方で，画像データの容易な改竄をも可能としている。
【０００３】従来の紙文化では，書類や請求書に改竄が行われていないこと，すなわち，原本性を保証するために，印章（マークなども含む）やサインなどが用いられていた。また，紙幣や商品券，あるいは公的書面などのように，透かしを用いてその原本性を保証することも行われている。この点，上述のペーパーレス対策を講じるに当たっても，書類や請求書の原本性を保証するための何らかの対策を講じる必要がある。
【０００４】画像データの場合，電子的な処理を行えば，視覚的に何ら痕跡を残さずにその一部を改竄することが比較的容易に行える。このため，紙文化の場合のように，単にマークやサインなどを画像データの一部に重ね合わせることのみでは原本性を保証することは難しい。そこで従来より，画像を符号化したデータからハッシュ値を得ることや，画像を符号化したデータに電子透かしを組み込むことで，原本性を保証することが行われている。かかるハッシュ値や電子透かしを用いれば，画像データの一部にでも改竄が行われた場合，画像データの復号の際にその改竄の有無を判断することができる。
【０００５】
【発明が解決しようとする課題】ところで，紙文化における印章やサイン，あるいは透かしの場合には，何人もこれを視覚的に確認でき，改竄が行われていないこと（原本性）を容易かつ即座に判断することができる。しかしながら，上述のペーパーレス対策におけるハッシュ値や電子透かしを用いた電子的な処理を用いた場合には，画像データの改竄有無を判断するためには，復号器の操作等の特別な処理が必要であり，容易に判断を行えるものではなかった。
【０００６】また，電子透かしを用いた場合，電子透かしを埋め込むアルゴリズムを解析されてしまうと，任意の画像データに対してひとたび画像データを改竄した後に，そのアルゴリズムにより電子透かしを埋め込まれてしまうおそれがある。画像データに電子透かしが埋め込まれているということは，すなわち，その画像データに改竄が行われていないことを保証することであるため，却って，電子透かし技術が画像データの改竄の発見を困難にするという結果となる。
【０００７】本発明は，従来の画像データの改竄防止方法が有する上記問題点に鑑みてなされたものであり，本発明の目的は，画像データの改竄を容易に防止でき，画像データの原本性を視覚的に確認することの可能な，新規かつ改良された画像伝送装置及び画像受信装置を提供することである。
【０００８】
【課題を解決するための手段】上記課題を解決するため，本発明によれば，請求項１に記載のように，画像伝送装置において，第１の画像を符号化する第１の画像符号化手段と，前記第１の画像のハッシュ値を計算するハッシュ値演算手段と，第２の画像を符号化する第２の画

像符号化手段と，前記第２の画像の符号化データを，前記第１の画像のハッシュ値をキーとして暗号化する暗号化手段と，前記第１の画像の符号化データと前記暗号化された第２の画像の符号化データとを伝送する伝送手段と，を有することを特徴とする，画像伝送装置が提供される。ここで，第２の画像とは，第１の画像の原本性を保証するために用いられる画像であり，例えば，請求項３に記載のように，マークを含む印章あるいはサインの画像である。

【０００９】第１の画像の符号化データと暗号化された第２の画像の符号化データは，別々のデータとして伝送するようにしてもよいが，請求項２に記載のように，前記伝送手段に，前記第１の画像の符号化データと前記暗号化された第２の画像の符号化データとを多重化する多重化手段を備えるようにし，多重化データとして伝送することが好ましい。データ伝送の制御を容易に行えるとともに，データ量の軽減によるネットワーク資源の軽減化を図ることが可能である。

【００１０】また，請求項４によれば，画像受信装置において，第１の画像の符号化データと暗号化された第２の画像の符号化データとを受信する受信手段と，前記第１の画像の符号化データを復号する第１の画像復号化手段と，前記復号された第１の画像のハッシュ値を計算するハッシュ値演算手段と，前記暗号化された第２の画像の符号化データを，前記第１の画像のハッシュ値をキーとして解読する暗号解読手段と，前記解読された第２の画像の符号化データを復号する第２の画像復号化手段と，前記復号された第１の画像と前記復号された第２の画像とを結合する画像結合手段と，を備えたことを特徴とする，画像受信装置が提供される。ここで，第２の画像とは，第１の画像の原本性を保証するために用いられる画像であり，例えば，請求項６に記載のように，マークを含む印章あるいはサインの画像である。

【００１１】なお，画像の符号化データと暗号化されたマーク画像の符号化データが多重化されたデータとして受信される場合を考慮すると，請求項５に記載のように，前記受信手段に，多重化データを分離する多重化分離手段を備えるようにし，多重化データを受信できる機能を付加することが好ましい。

【００１２】かかる画像伝送装置及び画像受信装置によれば，画像の一部にでも改竄が行われた場合，その改竄が行われた画像のハッシュ値は，改竄が行われていない画像のハッシュ値とは異なったものになる。このため，画像の一部にでも改竄が行われた場合，そのハッシュ値をキーとして解読されたマーク画像の符号化データは，改竄が行われていない場合の符号化データとは異なったものとなる。このため，最終的に生成される画像のマーク画像を見れば，画像に改竄が行われたか否かを視覚的かつ容易に確認することができる。

【００１３】

【発明の実施の形態】以下に添付図面を参照しながら，本発明にかかる画像伝送装置及び画像受信装置の好適な実施の形態について詳細に説明する。なお，本明細書及び図面において，実質的に同一の機能構成を有する構成要素については，同一の符号を付することにより重複説明を省略する。また，以下の説明において，マーク画像とは，印章（マークなどを含む）あるいはサインの画像とする。

【００１４】（画像伝送装置１０）まず，画像伝送装置の一実施形態を，図１を参照しながら説明する。画像伝送装置１０は，図１に示したように，画像Ａ０を符号化する画像符号化手段１０１と，画像Ａ０のハッシュ値Ｈを計算するハッシュ値演算手段１０２と，マーク画像Ｂ０を符号化するマーク画像符号化手段１０３と，マーク画像の符号化データＢ１を，画像Ａ０のハッシュ値Ｈをキーとして暗号化する暗号化手段１０４と，画像の符号化データＡ１と暗号化されたマーク画像の符号化データＢ２とを多重化して伝送する多重化手段１０５とを備えている。

【００１５】画像符号化手段１０１は，画像入力端子１より入力された画像Ａ０を符号化する手段である。ここでの符号化は，ＪＰＥＧ（Ｊｏｉｎｔ Ｐｈｏｔｏｇｒａｐｈｉｃ Ｃｏｄｉｎｇ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ），ＪＢＩＧ（ＪｏｉｎｔＢｉ－ｌｅｖｅｌ Ｉｍａｇｅ Ｃｏｄｉｎｇ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ）などの，カラー／２値静止画像の符号化の国際標準などが用いられる。

【００１６】ハッシュ値演算手段１０２は，入力された画像Ａ０のハッシュ値Ｈを計算する手段である。ここでのハッシュ値の演算は，ＭＤ５（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ ５）やＤＳＡ（Ｄｅｓｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ）などが用いられる。

【００１７】マーク画像符号化手段１０３は，マーク画像入力端子２より入力されたマーク画像Ｂ０を符号化する手段である。ここでの符号化は，画像化符号化手段１０１と同様に，ＪＰＥＧ，ＪＢＩＧなどの，カラー／２値静止画像の符号化の国際標準などが用いられる。あるいは，画像伝送装置１０内に，一の画像符号化手段のみを備えるように構成し，この一の画像符号化手段により，画像Ａ０及びマーク画像Ｂ０の符号化を併せて行うようにしてもよい。

【００１８】暗号化手段１０４は，ハッシュ値演算手段１０２で得られたハッシュ値Ｈをキーとして，マーク画像符号化手段１０３によって符号化されたマーク画像の符号化データＢ１を，暗号化する。ここでの暗号化は，ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）やＴｒｉｐｌｅ ＤＥＳなど，共通鍵暗号方式が用いられる。

【００１９】伝送手段１０５では，画像符号化手段１０１により得られた画像の符号化データＡ１と，マーク画

像符号化手段１０３により得られた暗号化されたマーク画像の符号化データＢ２の多重化して伝送する。ここでの多重化は，ＪＢＩＧ２のように，異なる領域の画像データとして多重化する方法や，コメント領域にバイナリデータとして格納する方法などがある。

【００２０】なお，本実施の形態では，伝送手段１０６に，データを多重化する機能とデータを伝送する機能とを有する場合について説明するが，データを多重化する機能は必ずしも必須の機能ではなく，画像の符号化データＡ１と，暗号化されたマーク画像の符号化データＢ２とを別のデータとして伝送するようにしてもよい。

【００２１】次いで，上述のように構成される画像伝送装置１０の動作について，データの遷移の観点から，図２を参照しつつ説明する。

【００２２】画像入力端子１より入力された画像Ａ０は，ハッシュ値演算手段１０２によってハッシュ値Ｈが計算されるとともに，画像符号化手段１０１によって符号化される。一方，マーク画像入力端子２より入力されたマーク画像Ｂ０は，マーク画像符号化手段１０３によって符号化される。

【００２３】マーク画像符号化手段１０３によって符号化されたマーク画像の符号化データＢ１は，ハッシュ値演算手段１０２で得られたハッシュ値Ｈをキーとして，暗号化される。

【００２４】画像の符号化データＡ１と，暗号化されたマーク画像の符号化データＢ２は，伝送手段１０５によって多重化され，符号化データＣとして，データ出力端子３より出力される。

【００２５】（画像受信装置２０）次いで，画像受信装置の一実施形態を，図３を参照しながら説明する。なお，本実施の形態では，画像受信装置２０は，上記画像伝送装置１０が伝送するデータＣを受信するものとして説明する。

【００２６】画像受信装置２０は，図３に示したように，画像伝送装置１０が伝送する符号化データＣを受信し，この符号化データＣを，画像の符号化データＡ１と暗号化されたマーク画像の符号化データＢ２とに分離する受信手段１０６と，画像の符号化データＡ１を復号する画像復号手段１０７と，復号された画像Ａ０のハッシュ値Ｈを計算するハッシュ値演算手段と，暗号化されたマーク画像の符号化データＢ２を，画像Ａ０のハッシュ値Ｈをキーとして解読する暗号解読手段１０９と，解読されたマーク画像の符号化データＢ１を復号するマーク画像復号化手段１１０と，復号された画像Ａ０と復号されたマーク画像Ｂ０とを結合する画像結合手段１１１とを備えている。

【００２７】受信手段１０５では，画像伝送装置１０のデータ出力端子３より伝送された符号化データＣを受信し，この符号化データＣを，画像の符号化データＡ１と暗号化されたマーク画像の符号化データＢ２とに分離する。なお，本実施の形態では，画像受信装置２０は，多重化された符号化データＣを受信し，この多重化データを分離する機能を有する場合について説明するが，画像の符号化データＡ１と暗号化されたマーク画像の符号化データＢ２とが別のデータとして伝送される場合には，受信手段１０５には，多重化データを分離する機能は必ずしも必須の機能ではない。

【００２８】画像復号化手段１０７は，受信手段１０６で得られた画像の符号化データＡ１を復号化する手段である。ここでの復号化は，上記画像伝送装置１０内の画像符号化手段１０１に対応した機能であるものとし，符号化データＡ１を復号化して画像Ａ０を得る。

【００２９】ハッシュ値演算手段１０８は，画像復号化手段１０７で得られた画像Ａ０のハッシュ値Ｈを計算する。ここでのハッシュ値の演算は，上記画像伝送装置１０内のハッシュ値演算手段１０１と同様に，ＭＤ５（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ５）やＤＳＡ（Ｄｅｓｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ）などが用いられる。

【００３０】暗号解読手段１０９は，受信手段１０６で得られた暗号化されたマーク画像の符号化データＢ２を，ハッシュ値演算手段１０８より得られたハッシュ値Ｈをキーとして，解読する。ここでの暗号解読は，上記画像伝送装置１０内の暗号化手段１０４に対応した機能であるものとし，暗号化されたマーク画像の符号化データＢ２を解読してマーク画像の符号化データＢ１を得る。

【００３１】マーク画像復号化手段１１０は，暗号解読手段１０９で得られたマーク画像の符号化データＢ１を復号化する手段である。ここでの復号化は，上記画像伝送装置１０内のマーク画像符号化手段１０３に対応した機能であるものとし，マーク画像の符号化データＢ１を復号化してマーク画像Ｂ０を得る。

【００３２】画像結合手段１１１は，画像復号化手段１０７で得られた画像Ａ０と，マーク画像復号化手段１１０で得られたマーク画像Ｂ０を結合する手段である。ここでの結合方法は，ＡＮＤやＯＲ，加算，置換などが用いられる。画像Ａ０とマーク画像Ｂ０が結合され得られた画像Ｄは，画像出力端子６より出力される。

【００３３】次いで，上述のように構成される画像受信装置２０の動作について，データの遷移の観点から，図４を参照しつつ説明する。

【００３４】データ入力端子４より入力されたデータＣは，多重化データの分離機能を有する受信手段１０６によって受信され，画像の符号化データＡ１と，暗号化されたマーク画像の符号化データＢ２とに分離される。

【００３５】画像の符号化データＡ１は，画像復号化手段１０７により復号化される。復号化された画像Ａ０は，ハッシュ値演算手段１０８によりハッシュ値Ｈが計算される。

【００３６】暗号化されたマーク画像の符号化データＢ２は，画像Ａ０のハッシュ値Ｈをキーとして，暗号解読される。暗号解読されたマーク画像の符号化データＢ１は，マーク画像復号化手段１１０により，復号化される。

【００３７】画像復号化手段１０７により復号化された画像Ａ０と，マーク画像復号化手段１１０により復号化されたマーク画像Ｂ０は，画像結合手段１１１によって結合（オーバーレイ，多層化）される。結合された画像Ｄは，画像出力端子６より出力される。

【００３８】図４に示した例では，画像Ａ０に改竄が行われておらず，ハッシュ値Ｈが正しいものであるため，出力画像Ｄには，正しいマーク画像が表示されている。画像Ａ０の一部にでも改竄が行われていた場合，ハッシュ値演算の性格上，ハッシュ値演算手段１０８は異なるハッシュ値Ｈ’を算出する。このハッシュ値Ｈ’を暗号鍵として解読され，復号化されたマーク画像は，正しいマーク画像Ｂ０とは異なった画像（ノイズ）となるか，あるいは復号化が正常に行われず，マーク画像を得ることができない。このようにして，画像の原本性を視覚的かつ容易に確認することができるのである。

【００３９】以上説明したように，本実施の形態にかかる画像伝送装置１０及び画像受信装置２０によれば，画像の一部にでも改竄が行われた場合，その改竄が行われた画像のハッシュ値は，改竄が行われていない画像のハッシュ値Ｈとは異なったものになる。このため，画像の一部にでも改竄が行われた場合，そのハッシュ値をキーとして解読されたマーク画像の符号化データは，改竄が行われていない場合の符号化データとは異なったものとなる。このため，最終的に生成される画像のマーク画像を見れば，画像に改竄が行われたか否かを視覚的かつ容易に確認することができる。

【００４０】以上，添付図面を参照しながら本発明にかかる画像伝送装置及び画像受信装置の好適な実施形態について説明したが，本発明はかかる例に限定されない。当業者であれば，特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり，それらについても当然に本発明の技術的範囲に属するものと了解される。

【００４１】

【発明の効果】以上説明したように，本発明によれば，画像データの改竄を容易に防止でき，画像データの原本性を視覚的に確認することが可能である。

【図面の簡単な説明】

【図１】画像伝送装置の一実施形態を示す説明図である。

【図２】図１の画像伝送装置におけるデータの遷移を示す説明図である。

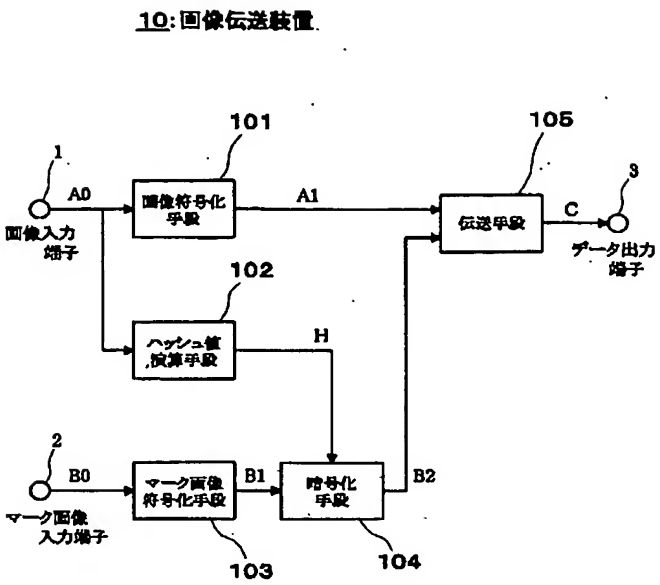
【図３】画像受信装置の一実施形態を示す説明図である。

【図４】図３の画像受信装置におけるデータの遷移を示す説明図である。

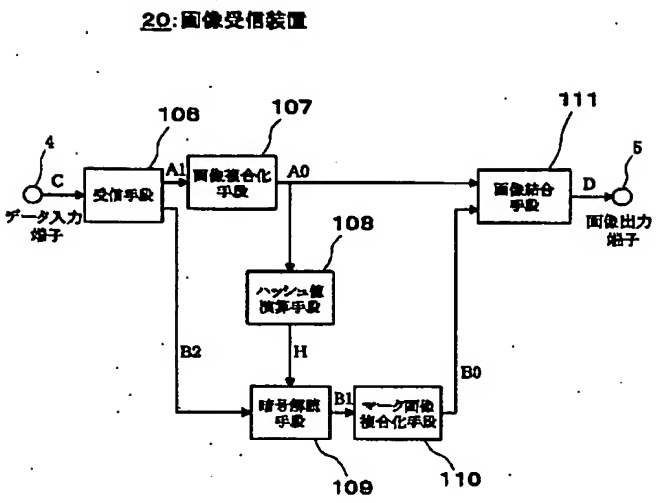
【符号の説明】

１０　画像伝送装置
１　画像入力端子
２　マーク画像入力端子
１０１　画像符号化手段
１０２　ハッシュ値演算手段
１０３　マーク画像符号化手段
１０４　暗号化手段
１０５　伝送手段
３　データ出力端子
２０　画像受信装置
４　データ入力端子
１０６　受信手段
１０７　画像符号化手段
１０８　ハッシュ値演算手段
１０９　暗号解読手段
１１０　マーク画像符号化手段
１１１　画像結合手段
６　画像出力端子

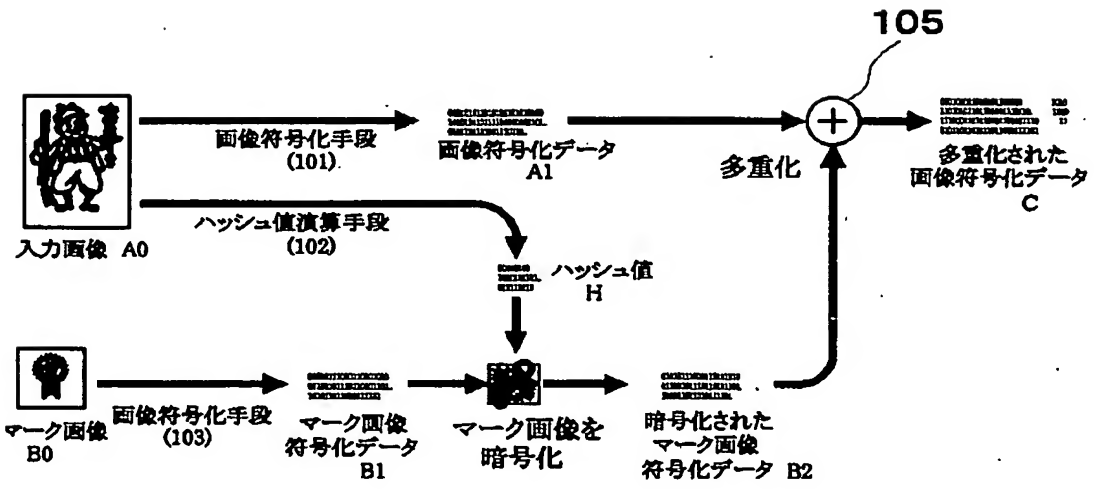
【図１】


10:画像伝送装置
1
画像入力端子
A0
101
画像符号化手段
A1
105
伝送手段
C
3
データ出力端子
102
ハッシュ値演算手段
H
2
マーク画像入力端子
B0
マーク画像符号化手段
B1
暗号化手段
B2
103
104

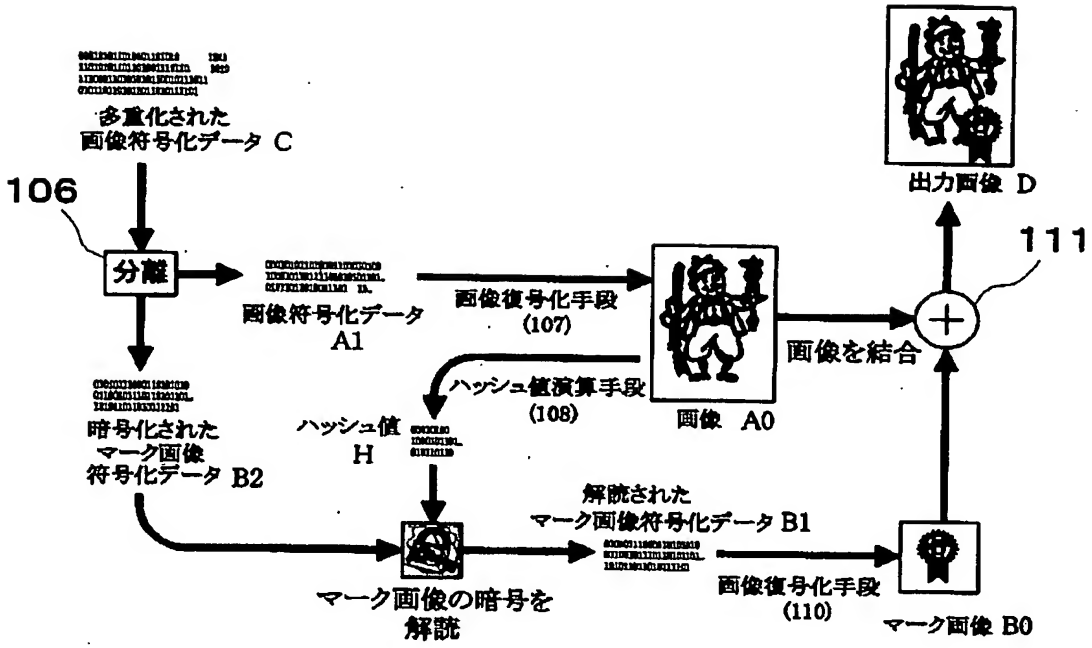
【図３】


20:画像受信装置
4
データ入力端子
C
106
受信手段
A1
107
画像複合化手段
A0
111
画像統合手段
D
5
画像出力端子
108
ハッシュ値演算手段
H
B2
B0
暗号復号手段
B1
マーク画像複合化手段
109
110

【図２】


105
画像符号化手段
(101)
画像符号化データ
A1
多重化
多重化された
画像符号化データ
C
入力画像 A0
ハッシュ値演算手段
(102)
ハッシュ値
H
マーク画像
B0
画像符号化手段
(103)
マーク画像
符号化データ
B1
マーク画像を
暗号化
暗号化された
マーク画像
符号化データ B2

【図４】


多重化された
画像符号化データ C
106
分離
画像符号化データ
A1
画像復号化手段
(107)
画像 A0
出力画像 D
111
画像を結合
ハッシュ値演算手段
(108)
暗号化された
マーク画像
符号化データ B2
ハッシュ値
H
解読された
マーク画像符号化データ B1
マーク画像の暗号を
解読
画像復号化手段
(110)
マーク画像 B0